Cont B2

(b) verifying said binding using a cryptographic verification key associated with a trusted party performing said binding; and

(c) using said financial account datum to authorize a transaction order digitally signed by said user with a private key corresponding to said public key.

Sub C1

3. The method of claim 2 where said digital certificate constitutes said binding.

4. The method of claim 2 where said binding is embedded in said digital certificate.

5. The method of claim 2 where said financial account datum includes a credit card number.

A1

6. The method of claim 2 where said financial account datum includes a debit card number.

7. The method of claim 2 where said financial account datum includes a PIN.

8. The method of claim 2 where said financial account datum includes a card verification value 2.

9. The method of claim 2 where said financial account datum includes checking account information.

10. The method of claim 2 where said binding is performed with a symmetric key shared between said trusted party and a party performing said verification step.

11. The method of claim 2 where said binding is performed with an asymmetric key corresponding to said cryptographic verification key.

12. The method of claim 2 where said binding is performed by an issuer of said digital certificate.

C1

~~13. The method of claim 2 where said binding is perform by an issuer of said financial accounting datum.~~

~~14. The method of claim 2 where said digital certificate is protected with an access code known to said user.~~

Sub B3

A1

~~15. A method for providing electronic payment capabilities to a user in a networked computer environment, comprising the steps of:~~

~~(a) obtaining a financial account datum associated with said user;~~

~~(b) obtaining a public key associated with said user;~~

~~(c) obtaining a cryptographically assured binding of said public key to at least a portion of said financial account datum,~~

~~(i) said binding being conveyed in a digital certificate for said user,~~

~~(ii) said digital certificate being usable by said user to conduct an electronic transaction involving said financial account datum; and~~

~~(d) transmitting said digital certificate to said user, enabling said user to conduct said electronic transaction involving (i) a merchant from whom at least a portion of said financial account datum is kept confidential, and (ii) a transaction processor capable of verifying said binding using a cryptographic verification key associated with a trusted party performing said binding.~~

Sub C1

~~16. The method of claim 15 where said digital certificate constitutes said binding.~~

~~17. The method of claim 15 where said binding is embedded in said digital certificate.~~

~~18. The method of claim 15 where said financial account datum includes a credit card number.~~

~~19. The method of claim 15 where said financial account datum includes a debit card number.~~

20. ~~The method of claim 15 where said financial account datum includes a PIN.~~

21. ~~The method of claim 15 where said financial account datum includes a card verification value 2.~~

22. ~~The method of claim 15 where said financial account datum includes checking account information.~~

C1

A1

23. ~~The method of claim 15 where said binding is performed with a symmetric key shared between said trusted party and said transaction processor.~~

24. ~~The method of claim 15 where said binding is performed with an asymmetric key corresponding to said cryptographic verification key.~~

25. ~~The method of claim 15 where said binding is performed by an issuer of said digital certificate.~~

26. ~~The method of claim 15 where said binding is performed by an issuer of said financial account information.~~

27. ~~The method of claim 15 further comprising the step, after step (a), of verifying said financial account datum.~~

28. ~~The method of claim 15 where said digital certificate is protected with an access code known to said user.~~

29. ~~The method of claim 15 where said digital certificate is stored at a credential server accessible to said user.~~

Sub B4

30. An apparatus for authorizing an electronic purchase in a networked computer environment, comprising:

(a) a computer processor;

(b) a memory connected to said processor storing a program to control the operation of said processor;

(c) the processor operable with said program in said memory to:

(i) receive, from a merchant, a transaction authorization request, said request including a digital certificate passed through said merchant from a user involved in said transaction,

(1) said digital certificate including financial account datum associated with said user, at least a portion of which datum is confidential from said merchant,

(2) said digital certificate conveying a binding between at least a portion of said financial account datum and a public key of said user;

(ii) verify said binding using a cryptographic verification key associated with a trusted party performing said binding; and

(iii) use said financial account datum to authorize a transaction order digitally signed by said user with a private key corresponding to said public key.

A1 B4

Sub C1

31. The apparatus of claim 30 where said financial account datum includes a PIN.

32. The apparatus of claim 30 where said financial account datum includes a card verification value 2.

33. The apparatus of claim 30 where said binding is performed with an asymmetric key corresponding to said cryptographic verification key.

Sub B5

34. An apparatus for providing electronic payment capabilities to a user in a networked computer environment, comprising:

(a) a processor;

(b) a memory connected to said processor storing a program to control the operation of said processor;

(c) the processor operable with said program in said memory to:

(i) obtain a financial account datum regarding said user,

(ii) obtain a public key associated with said user,

(iii) obtain a cryptographically assured binding of said public key to at least a portion of said financial account datum,

(1) said binding being conveyed in a digital certificate for said user,

(2) said digital certificate being usable by said user to conduct an electronic transaction involving said financial account datum, and

Cont B5

A1

(iv) transmit said digital certificate to said user, enabling said user to conduct said electronic transaction involving (1) a merchant from whom at least a portion of said financial account datum is kept confidential, and (2) a transaction processor capable of verifying said binding using a cryptographic verification key associated with a trusted party performing said binding.

35. The apparatus of claim 34 where said financial account datum includes a PIN.

Sub C1

36. The apparatus of claim 34 where said financial account datum includes a card verification value 2.

37. The apparatus of claim 34 where said binding is performed with an asymmetric key corresponding to said cryptographic verification key.

Sub B4

38. A computer-readable storage medium encoded with processing instructions for implementing a method for authorizing an electronic purchase in a networked computer environment, said processing instructions for directing a computer to perform the steps of:

(a) receiving, from a merchant, a transaction authorization request, said request including a digital certificate passed through said merchant from a user involved in said transaction, cont'd B6

(i) said digital certificate including a financial account datum associated with said user, at least a portion of which datum is confidential from said merchant,

(ii) said digital certificate conveying a binding between at least a portion of said financial account datum and a public key of said user;

(b) verifying said binding using a cryptographic verification key associated with a trusted party performing said binding; and

(c) using said financial account datum to authorize a transaction order digitally signed by said user with a private key corresponding to said public key.

4! Sub C1

39. The computer-readable medium of claim 38 where said financial account datum includes a PIN.

40. The computer-readable medium of claim 38 where said financial account datum includes a card verification value 2.

41. The computer-readable medium of claim 38 where said binding is performed with an asymmetric key corresponding to said cryptographic verification key.

Sub B7

42. A computer-readable storage medium encoded with processing instructions for implementing a method for providing electronic payment capabilities to a user in a networked computer environment, said processing instructions for directing a computer to perform the steps of:

(a) obtaining a financial account datum regarding said user;

(b) obtaining a public key associated with said user;

(c) obtaining a cryptographically assured binding of said public key to at least a portion of said financial account datum,

(i) said binding being conveyed in a digital certificate for said user,

(ii) said digital certificate being usable by said user to conduct an electronic transaction involving said financial account datum; and cont B7

(d) transmitting said digital certificate to said user, enabling said user to conduct said electronic transaction involving (i) a merchant from whom at least a portion of said financial account datum is kept confidential, and (ii) a transaction processor capable of verifying said binding using a cryptographic verification key associated with a trusted party performing the said binding.

Sub C1

43. The computer-readable medium of claim 42 where said financial account datum includes a PIN.

A1

44. The computer-readable medium of claim 42 where said financial account datum includes a card verification value 2.

45. The computer-readable medium of claim 42 where said binding is performed with an asymmetric key corresponding to said cryptographic verification key.

Sub B8

46. A digital certificate for use in an electronic payment transaction in a networked computer environment, comprising:

(a) a financial account datum associated with a user, at least a portion of which datum is confidential from a merchant involved in said payment transaction;

(b) a cryptographically assured binding of a public key associated with said user to at least a portion of said financial account datum, said binding having been generated with a cryptographic verification key associated with a trusted party performing said binding;

(c) said digital certificate configured for use by a transaction processor to:

(i) verify said binding using a cryptographic verification key associated with said trusted party, and

(ii) access said financial account datum to authorize a transaction order digitally signed with said user's private key corresponding to said public key.

47. The digital certificate of claim 46 where said digital certificate constitutes said binding.

48. ~~The digital certificate of claim 46 where said binding is embedded in said digital certificate.~~

49. ~~The digital certificate of claim 46 where said financial account datum includes a credit card number.~~

50. ~~The digital certificate of claim 46 where said financial account datum includes a debit card number.~~

51. ~~The digital certificate of claim 46 where said financial account datum includes a PIN.~~

52. ~~The digital certificate of claim 46 where said financial account datum includes a card verification value 2.~~

53. ~~The digital certificate of claim 46 where said financial account datum includes checking account information.~~

54. ~~The digital certificate of claim 46 where said binding is performed with a symmetric key shared between said trusted party and said transaction processor.~~

55. ~~The digital certificate of claim 46 where said binding is performed with an asymmetric key corresponding to said cryptographic verification key.~~

56. ~~The digital certificate of claim 46 where said binding is performed by an issuer of said digital certificate.~~

57. ~~The digital certificate of claim 46 where said binding is performed by an issuer of said financial account datum.~~